EXHIBIT 26

ORACLE® **11**^{g}
DATABASE

An Oracle White Paper
March 2011

Defense In-Depth Security for Oracle Siebel Applications

ORACLE®

Executive Overview

Applications play a critical role in the day to day operations of nearly every organization worldwide. For that reason organizations have historically focused on the high availability and scalability aspects of applications for business continuity. Today, however, safeguards must be deployed that help protect against information security threats. These threats directly impact such business initiatives as application consolidation and outsourcing. Oracle database security solutions are focused on protecting sensitive data through a defense-in-depth architecture. This means securing the application roles and protecting the application data and structure through database-enforced change controls, providing preventive controls on privileged user access to application data, encrypting sensitive data, and permanently masking sensitive data when moved from production to test environment. To help Oracle Siebel customers protect their sensitive data and applications, Oracle has pre certified Oracle database security solutions such as Oracle Database Vault and Oracle Advanced Security with Oracle Siebel.

Oracle Advanced Security with Oracle Siebel

Industry directives such as the Payment Card Industry Data Security Standard (PCI-DSS) and numerous state privacy breach notification laws require the use of encryption for sensitive data. Oracle Advanced Security provides a transparent and scalable encryption solution for encrypting sensitive Oracle Siebel application data in the database, on the network, and on disk backup. As the definition of sensitive data continues to expand far beyond credit card and social security numbers, Oracle Advanced Security provides the flexibility to encrypt individual columns or the entire application data.

"Our aim is to have the most secure database systems in our industry which protect our client data and our business from internal and external threats. The Oracle security components underpinning our standard Oracle security configuration bring a new level of assurance to our senior management and audit teams."

—— Akash Gharu, Global Database Services Manager, CMC Markets

Transparent Data Encryption with Oracle Siebel

Oracle Advanced Security transparent data encryption (TDE) automatically encrypts Oracle Siebel application data when written to database files and transparently decrypts the data when accessed inside the database. TDE encrypts sensitive Siebel Application data without requiring any application code changes. Traditional access controls still apply, so data will not be decrypted until an application or database user has authenticated to the Oracle database and passed all access control checks including those enforced by Oracle Database Vault. Encrypted data remains secure in the event of unauthorized access to files at the operating system level, discarded disk drives and off-site disk backup. TDE column encryption can be used to protect individual columns in application tables containing credit card numbers or other personally identifiable information (PII). Encryption of credit card numbers stored in Oracle Siebel applications helps organizations comply with section 3.6 of the PCI Data Security Standard (PCI-DSS). Customers running on Oracle Database 11g can use TDE tablespace encryption to protect all the application tablespaces.

Supported Oracle Siebel Releases

All Oracle Siebel application releases 7.7+, 7.8+, and 8.0+ are supported with Oracle Transparent *Column* Encryption. Oracle Siebel release 8.0+ is supported with Oracle Transparent *Tablespace* Encryption.

For more information:

Oracle Tablespace Encryption for Siebel Data Sheet[1]
Transparent Data Encryption best practices [2]

---

[1] http://www.oracle.com/technetwork/database/security/ds-advanced-security-tde-sebl-134242.pdf

[2] http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf

2

Oracle Database Vault with Oracle Siebel

"With Oracle Database Vault and the Transparent Data Encryption feature provided by Oracle Advanced Security, our highly sensitive personal and medical data is now protected against unauthorized access. We therefore were able to integrate our national health information system with healthcare providers' local information systems."

— Madis Tiik, Member of Management Board, Estonian eHealth Foundation

Oracle Database Vault enforces strong operational controls inside the Oracle database creating a highly secure environment for Oracle Siebel applications. Oracle Database Vault realms prevent ad hoc access to application data by privileged users. Oracle Database Vault realms are essentially firewalls inside the Oracle database, blocking all encompassing DBA like privileges from being used to access Oracle Siebel application data. Oracle Database Vault realms are transparent to existing applications, enabling significantly stronger security controls to be achieved without changing the existing application code or performing a tedious least privilege exercise.

Oracle Database Vault command rules significantly tighten security by limiting who, when, where and how databases, data and applications can be accessed. Multiple factors such as IP address, time of day and authentication method can be used in a flexible and adaptable manner to enforce access controls regardless of whether the connection is local or remote and without making changes to the application. For example, access can be restricted to a specific middle tier, creating a "trusted-path" to the application data and preventing use of unauthorized ad hoc tools, local or remote, to access the Oracle database. Policies can be associated with many SQL commands including data definition language (DDL) commands such as *create*, *drop* and *truncate* table.

Oracle Database Vault enforces separation of duty by providing three distinct responsibilities out-of-the-box for: security, account management, and day-to-day database administration activities. For example, Oracle Database Vault blocks a DBA from creating a new user in the database even though the DBA has the *create user* privilege granted through the DBA role. This capability locks down and prevents unauthorized changes that may result in unexpected audit findings as well as potential security vulnerabilities such as creating an un-authorized DBA account in the database.

Oracle Database Vault security controls address common requirements found in regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and the Health Insurance Portability and Accountability Act (HIPAA). These regulations require strong internal controls to protect sensitive data such as financial, healthcare, and credit card information. Outsourcing and off-shoring, application consolidation, and increasing concerns over insider threats have resulted in an almost mandatory requirement for strong controls on access to sensitive application data. Oracle Database Vault enforces real-time preventive controls in the Oracle Database supporting the Oracle Siebel applications.

3

Oracle Database Vault protections for Oracle Siebel enables customers to restrict privileged users' access to application data, enforce separation-of-duty, and provide tighter access control with multi-factor authorization.

Supported Oracle Siebel Releases

All Siebel application modules and all Siebel application releases 7.7 or higher are supported with

Oracle Database Vault. Oracle Database release 10.2.0.4 or higher, and Oracle Database 11.1.0.7 or

higher are supported with this certification.

For more information:

Oracle Database Vault security policies for Oracle Siebel Applications[3]
Oracle Database Vault Certification with Oracle Siebel Applications Datasheet[4]

Oracle Data Masking for Oracle Siebel Applications

Enterprises have always shared data within and outside their organizations for various business purposes. Database administrators (DBAs) in these enterprises copy production data into staging or test environments to allow in-house developers or offshore testers to perform application development and application testing. The problem with data sharing is that copies of production data often contain company confidential, sensitive or personally identifiable information (PII), access to which is restricted by government regulations. Therefore, these enterprises run the risk of exposing sensitive information when sharing production data with application developers or software quality testers.

Oracle Data Masking Pack helps Oracle Siebel Applications customers achieve security and compliance by permanently obfuscating sensitive data in the production databases before they move to test environments. Oracle Data Masking Pack helps reduce security risks by irreversibly replacing the original Oracle Siebel sensitive data with fictitious data so that it can be shared safely with IT developers or offshore business partners. Oracle Data Masking Pack helps maintain the integrity of the Oracle Siebel applications while masking data.

Conclusion

Applications play a critical role in the day to day business operations and protecting those applications from information security threats has never been more important. While Oracle Siebel application

---

[3] http://www.oracle.com/technetwork/database/options/database-vault/index-090593.html

[4] http://www.oracle.com/technetwork/database/security/ds-database-vault-siebel-133249.pdf

4

level security ensures application users have access to the appropriate roles and responsibilities within the Oracle Siebel applications, threats today will attempt to bypass application controls to get to valuable data in the database. Oracle database security solutions are focused on protecting sensitive data through defense in-depth architecture. This means securing the application roles and protecting the application data and structure through database-enforced change controls, preventive controls on administrative access to application data, encryption of sensitive data, and masking sensitive application data.

ORACLE®

Oracle is committed to developing practices and products that help protect the environment

White Paper Title
March 2011
Author: Anna Leyderman
Contributing Authors: Kamal Tbeileih, Peter Wahl

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Hardware and Software, Engineered to Work Together

ORCLRS0811865